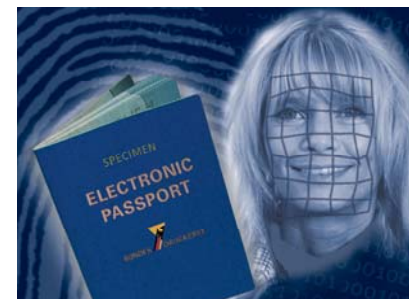
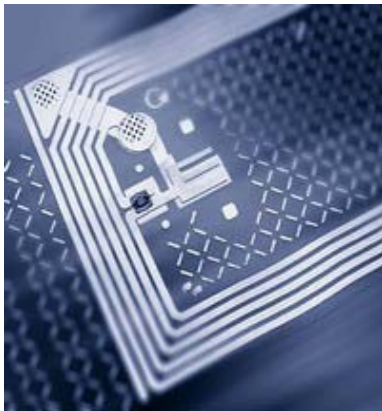


Autentizace v příkladech I



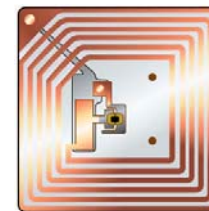
[Zkouška]

- Přejeme úspěšné nastudování a složení zkoušky
- Polosemestrálka 30 % bodů
- Finální písemka 70 % bodů
 - Uzavřené otázky
 - Otevřené otázky

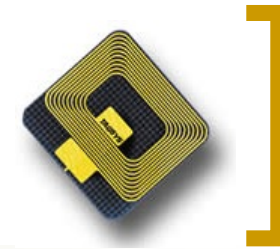


Bezdrátová technologie RFID

- RFID – Radio Frequency Identification
 - určeno k automatické identifikaci objektů
 - umožňuje přenos dat pomocí elektromagnetického pole
- Základní rozdělení RFID tagů (kromě R/O a R/W)
 - pasivní – bez vlastního zdroje energie
 - velmi malé (bez antény 0,15 mm × 0,15 mm) a tenké (7,5 μm)
 - levné a téměř neomezená životnost (není limitována baterií)
 - dosah max. několik metrů (v závislosti na frekvenci a anténě)
 - aktivní – vlastní zdroj energie a větší paměť/výkon
 - mohou šířit svůj vlastní signál – tzv. majáky (beacons)
 - dražší, dosah desítky metrů, životnost baterie až 5 let
 - semi-aktivní (či semi-pasivní) – vlastní zdroj energie pouze pro napájení čipu => rychlejší odezva než pasivní tagy



[Bezpečnost RFID



- Bezkontaktní komunikace s RFID tagem většinou nevyžaduje přímou viditelnost
 - komunikační vlastnosti závisí na použitém frekv. pásmu
 - většina tagů pracuje na 13,56 MHz => nelze přechít na vzdálenost větší než 1 m
 - tagy pracující na 868/915MHz => vyžadují přímou viditelnost
 - v blízkosti čtečky vysílá jedinečný identifikátor (číselný kód)
 - EPC kód obsahuje další inf. (výrobce, typ produktu apod.)
- Bezpečnostní problémy RFID (předmětem výzkumu)
 - soukromí – problém sledování a inventarizace
 - ochrana tagů proti neautorizovanému čtení
 - autentizace – problém snadného falšování/padělání tagů
 - ochrana čteček proti padělaným tagům

[Techniky zajištění soukromí I]

- Deaktivace tagu (absolutní jistota)
 - typicky čtečkou a na místě, kde zákazník přebírá zboží
 - ne vždy lze použít (knihovny, obchody nevyužívající RFID)
- Pasivní či aktivní rušení
 - pasivní – princip Faradayovy klece (kovová síť či hliníková fólie brání průchodu rádiových signálů)
 - aktivní – použití speciálního rušícího zařízení (dlouhé rušení může být nelegální a pro okolní RFID nežádoucí)
- Měření vzdálenosti (pomocí poměru signál/šum)
 - pokus o vzdálené čtení => odvysílání nesprávných dat
- Využití prostředníka (nutná autentizace vůči tagu)

[Techniky zajištění soukromí II]

- Změna jedinečného identifikátoru
 - nepravidelná: jednorázové přeznačení (neeliminuje problém sledování) či smazání (ostatní data zůstanou)
 - pravidelná: malá množina pseudonymů (rozpozná je pouze autorizovaná čtečka) či přešifrovávání
- Selektivní blokování
 - identifikátory rozděleny dle 1. bitu na soukromé a veřejné
 - blokující RFID tag „ruší“ čtení soukromých identifikátorů
 - využívá antikolizního protokolu používaného čtečkou
 - ne vždy funguje spolehlivě (závisí na umístění)
 - po úpravě lze zneužít k úplnému blokování identifikátorů


Podrobnější informace lze nalézt na <http://www.rsasecurity.com/rsalabs/node.asp?id=2115> konkrétně v http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf

[Cestovní pasy]

- Pas je identifikační průkaz nutný k přechodu státních hranic (až na výjimky) =>
- Kontroluje se
 - zda je pas originál (vydaný příslušnou autoritou), a ne padělek
 - tiskové technologie, vodoznak, prvky viditelné v UV světle ...
 - *digitální podpis dat, aktivní autentizace*
 - zda osoba, které jej předkládá, je osoba, již byl pas vydán (a ne někdo kdo pas našel, ukradl ...)
 - fotka oprávněného držitele
 - *biometrické údaje*
 - zda pas je stále platný (doba platnosti případně další omezení (lidé, po nichž je vyhlášeno pátrání, jimž bylo omezeno právo cestovat apod.))
 - policejní databáze (např. Interpol)
 - *automatizované čtení dat z pasu*



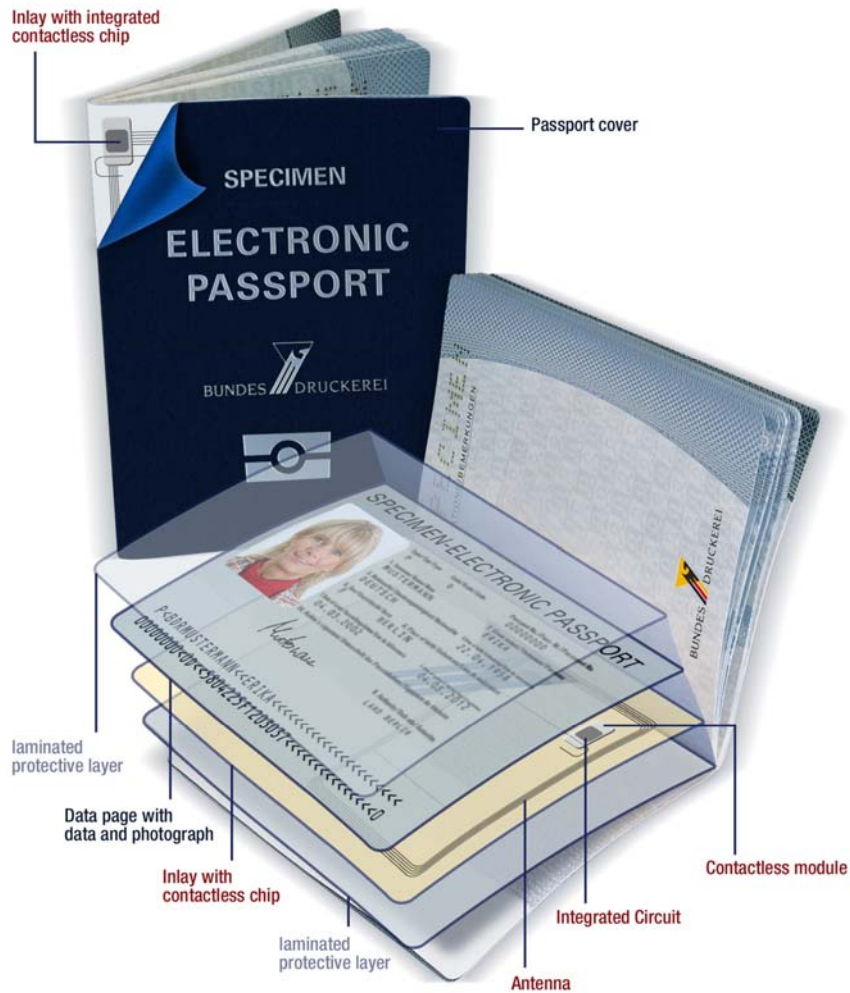
[ePasy – elektronické pasy]

- Pasy s vloženým RFID čipem
 - bezdrátová čipová karta podle ISO 14443 (A nebo B)
 - komunikace na 13,56 MHz
 - zamýšlený čtecí rozsah 0–10 cm
 - data uložena v 16 souborech (DG1 až DG16)
 - metadata v souboru EF.COM (verze + indikace, který z 16 DG je přítomen)
 - bezpečnostní soubor EF.SOD
- Na přední straně typicky označeny logem 



Obrázky ePasů převzaty z <http://www.bundesdruckerei.de/>

ePasy – další obrázky



► The contactless chip can be integrated into either the cover page or the data page.

[Pasivní autentizace]

- *Pasivní i aktivní autentizace do jisté míry podobná metodám SDA a DDA ve specifikaci EMV*
- Všechna data (každá datová skupina DG) jsou digitálně podepsána vydávající autoritou
 - soubor EF.SO_D obsahuje podepsané haše všech uložených DG
- Pro ověření podpisu je třeba mít k dispozici certifikát vydavatele
 - certifikační řetěz je obvykle uložen v pase
 - kořenové certifikáty nutné získat bezpečnou cestou (diplomatickou bilaterální výměnou)

[Pasivní autentizace]

The image shows two overlapping windows from a security management application. The background window is titled "LDSSecurityObject" and displays the configuration for a security object. The foreground window is titled "Certifikát" and shows the details of a selected certificate.

LDSSecurityObject

Version: 12159544

Hash algorithm

OID: { 2.16.840.1.101.3.4.2.1 }

Algorithm name: SHA-256

Parameters: 05 00 (NULL)

Hash values

- ✓ DG1: B1 C5 C6 5E 55 F0 C4 CA C6 E3 AD C0 9B 8C 13 73 26 E1 DF CF 44 F9 9C 10 EC 31 2E DF DF 1D 4A B0
- ✓ DG2: 8E 33 36 9A 87 60 0B 0E 6C 23 6D 27 2E 38 7C 79 A8 70 37 E2 5C C2 27 11 46 E6 E1 1E B2 CC 01 D0
- DG3: n/a
- DG4: n/a
- DG5: n/a
- DG6: n/a
- DG7: n/a
- DG8: n/a
- DG9: n/a
- DG10: n/a
- DG11: n/a
- DG12: n/a
- DG13: n/a
- DG14: n/a
- ✓ DG15: BE 7E 14 F7 EC F9 AD C4 D2 62 8E 39 6E 6E 91 6A 80 9E E7 61 98 80 1E 24 27 42 7A EB B6 BE CA CE
- DG16: n/a

Certifikát

Obecné | Podrobnosti | Cesta k certifikátu

Zobrazit: <Vše>

Pole	Hodnota
Verze	V3
Sériové číslo	01
Algoritmus podpisu	1.2.840.113549.1.1.11
Vystavitel	The Slovak CSCA, Department...
Platnost od	30. října 2007 10:06:18
Platnost do	2. února 2023 9:52:45
Předmět	The Slovak CSCA, Department...
Veřejný klíč	RSA (4096 Bits)

CN = The Slovak CSCA
OU = Department of CAs Operation
O = NSA of the Slovak Republic
L = Bratislava
C = SK

Upravit vlastnosti... Kopírovat do souboru...

OK

[Aktivní autentizace]

- Digitálně podepsaná data lze kopírovat (zkopírují se data včetně jejich podpisu)
- Snadnému kopírování se pasy mohou bránit aktivní autentizací
 - asymetrický pár klíče
 - soukromý klíč uložen v čipu, bez možnosti jeho přímého získání (čip je fyzicky bezpečný)
 - veřejný klíč je uložen v DG15 (tj., je digitálně podepsán)
 - protokol výzva-odpověď pro ověření, zda má pas k dispozici soukromý klíč
 - přečtu veřejný klíč pasu (DG15) a ověřím jeho podpis pomocí veřejného klíče vydávající autority
 - pošlu pasu náhodné číslo
 - pas náhodné číslo doplní svou náhodnou částí a podepíše
 - ověřím digitální podpis na základě veřejného klíče pasu

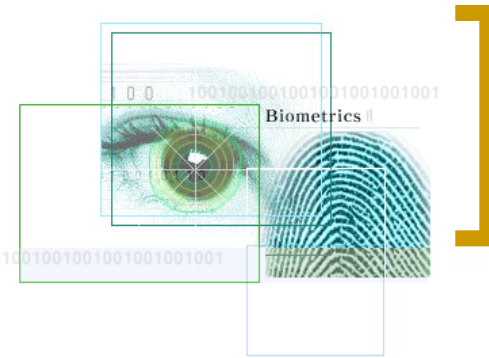
[Aktivní autentizace]

- Random challenge: E8 1E 4D FF 1E 4D 87 36
- Received response: C6 CB B4 96 B6 14 1E 84 44 27 AB 53
89 BB AE 43 DA 2E 1A 6F 10 F3 EC 9B 45 C6 2C F8 54 CD
79 B3 4E D8 4A 6C 98 96 86 7C 8E 00 B9 DE 2D 35 BA 11



96 85 44 4A 8E EB 87 31 0E AF
64 50 A6 E4 72 59 EF F8 AA 8F
14 6B CB 6A 1D 42 B4 58 59 72
D2 ED 42 11 EE 46 7C 90 E0 34
39 50 F4 1C D6 77 79 8C EC CD
F0 0F 8E A9 33 D2 B4 08 4A 92
81 87 44 26 34 5B C5 B5 57 84
6C 98 FF 78 E0 33 59 D3 CA 2A
90 00

[Biometriky



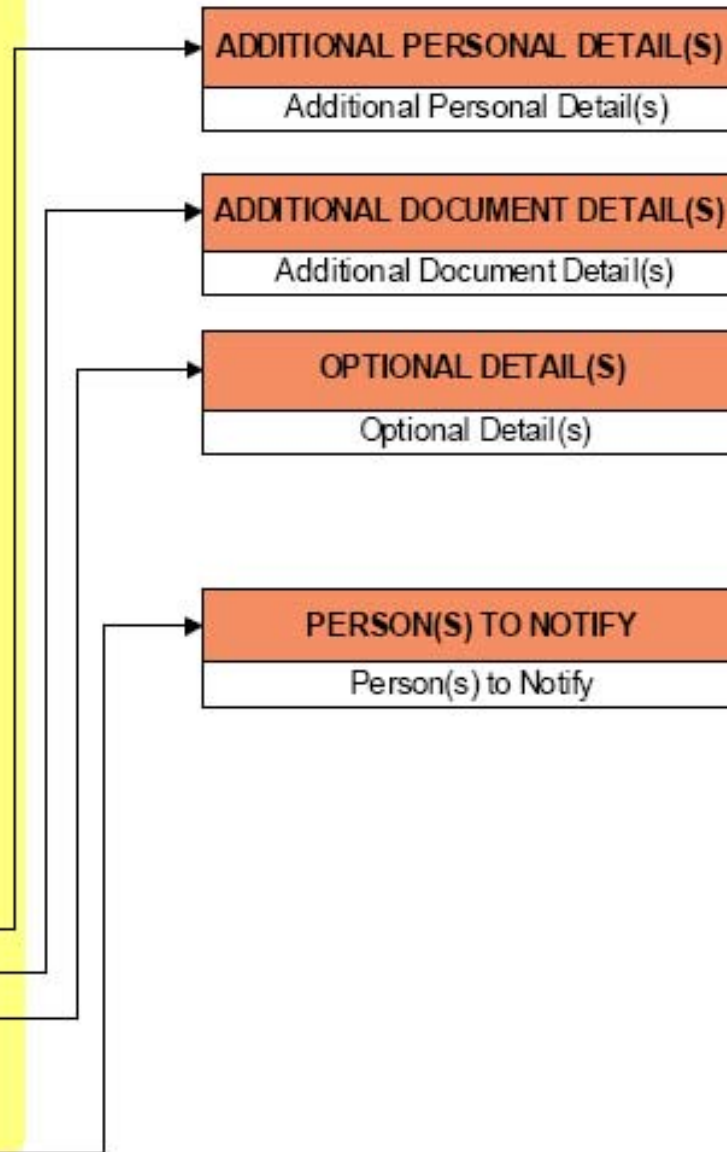
- Pro automatizovanou verifikaci identity předkladatele pasu (DG 2-4)
 - obličej (ve formátu JPEG/JPG2000 s případnými dalšími významnými biometrickými body, viz ISO 19794-5)
 - otisk prstu (obrázek WSQ nebo zpracovaná data ve formě markantů, vzorů apod., viz ISO 19794-2, 19794-3, 19794-4, 19794-8)
 - duhovka (obrázek viz ISO 19794-6)

- Dále jako digitální verze vytištěných dat (DG5-7)
 - fotografie držitele (viz ISO 10918)
 - podpis držitele (viz ISO 10918)

ISSUING STATE or ORGANIZATION RECORDED DATA

Detail(s) Recorded in MRZ	DG1	Document Type	
		Issuing State or organization	
		Name (of Holder)	
		Document Number	
		Check Digit - Doc Number	
		Nationality	
		Date of Birth	
		Check Digit - DOB	
		Sex	
		Date of Expiry or Valid Until Date	
		Check Digit - DOE/MUD	
		Optional Data	
		Check Digit - Optional Data Field	
		Composite Check Digit	
		Encoded Identification Feature(s)	GLOBAL INTERCHANGE FEATURE
Additional Feature(s)	DG3		Encoded Finger(s)
	DG4		Encoded Eye(s)
Displayed Identification Feature(s)	DG5	Displayed Portrait	
	DG6	Reserved for Future Use	
	DG7	Displayed Signature or Usual Mark	
Encoded Security Feature(s)	DG8	Data Feature(s)	
	DG9	Structure Feature(s)	
	DG10	Substance Feature(s)	
	DG11	Additional Personal Detail(s)	
	DG12	Additional Document Detail(s)	
	DG13	Optional Detail(s)	
	DG14	Reserved for Future Use	
	DG15	Active Authentication Public Key Info	
	DG16	Person(s) to Notify	

Struktura dat



[Ochrana dat]

- RFID umožňuje zjištění existence čipu i čtení dat z čipu na dálku
 - viz techniky zajišťující soukromí
 - u ePasů zatím pouze pasivní rušení/stínění
 - efektivní pouze pokud je pas uzavřen
 - navíc také logické omezení přístupu k datům
- Řízení přístupu k datům
 - základní řízení přístupu (BAC)
 - tajný klíč lze získat z dat v MRZ
 - rozšíření řízení přístupu (EAC)
 - explicitní autorizace pro přístup k citlivým datům

Základní řízení přístupu

- Z MRZ je třeba získat
 - číslo pasu
 - datum narození
 - datum vypršení platnosti
- Hašujeme SHA-1 a generujeme dva 3DES-2 klíče
- Podle ISO 11770-2 autentizujeme a ustavíme sdílený šifrovací klíč
 - následná komunikace je šifrovaná, což brání odposlechu přenášených dat
- Data používaná k odvození klíče mají teoretickou entropii $\pm 56/74$ bitů (v praxi však klesá ke 35 bitům)
 - odposlechneme-li úspěšnou komunikaci, lze hrubou silou zjistit klíče a přenášená data dešifrovat

[Rozšířené řízení přístupu (EAC)]

- Silnější řízení přístupu než BAC
 - založeno na opravdu tajných klíčích (ne jako BAC)
 - důležité pro ochranu citlivých biometrik
 - otisk prstu (v EU nejpozději od 28.6.2009), DG3
 - duhovka, DG4
 - pro ochranu dat, které není nutné zpřístupnit všem zemím
 - lze určit, které země budou mít přístup (získají certifikátu)

Rozšířené řízení přístupu

- Každá země zřídí CV (Country Verifying) CA
 - určuje vydáváním certifikátů, které další země budou mít přístup k citlivým biometrikám
 - certifikát CV CA uložen v pase (kořenový certifikát)
- Další země zřizují DV (Document Verifier) CA
 - certifikována od CV dalších zemí
 - země které chtějí získat přístup k biom. datům
 - vydává koncové certifikáty inspekčním zařízením
- Pas pak od CV CA ověřuje inspekční zařízení
 - řádně certifikovaný veřejný klíč => ověření znalosti soukromého klíče (výzva-odpověď) => přístup k datům
- Autentizace čipu i terminálu
 - Diffie-Hellman (PKCS#3 nebo eliptické křivky ISO 15946)

[Autentizace čipu]

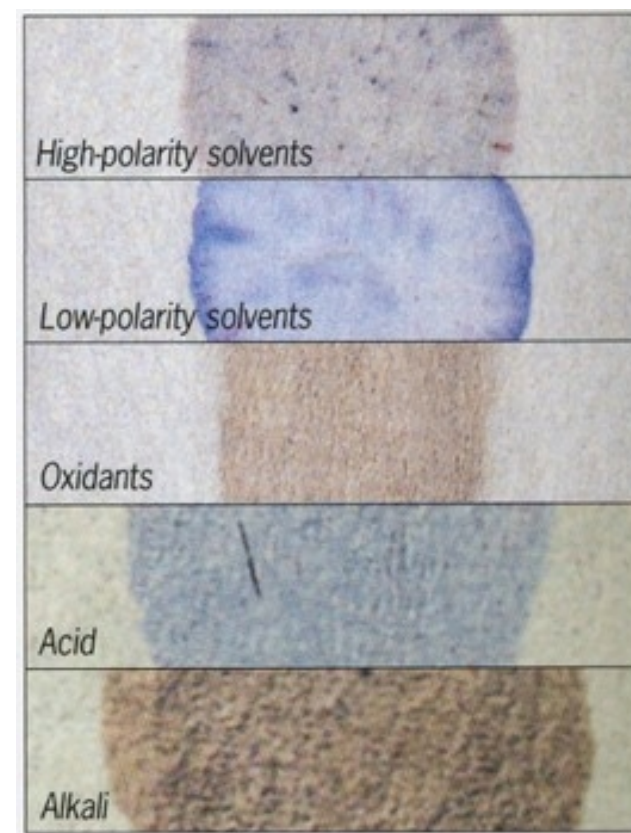
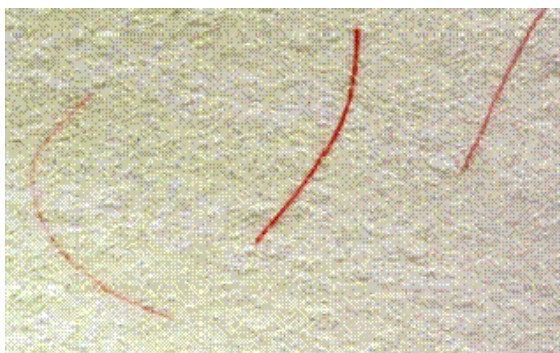
1. Terminál získá z pasu jeho veřejný DH_P
 - uložen digitálně podepsán v DG14
2. Terminál vygeneruje čerstvý dočasný DH_S pár
 - stejné doménové parametry jako klíčový pár čipu
 - pasu zašle veřejnou část
3. Odvození sdíleného klíče z DH_S (obě strany)
4. Ustavení nového šifrovaného kanálu namísto BAC
 - oproti BAC nyní již opravdu bezpečný (šifrování i MAC)
 - funkčně nahrazuje aktivní autentizaci
 - pas musí znát privátní část DH pro odvození klíče => test
 - aktivní autentizace stále podporována (systémy bez EAC)

[Autentizace terminálu]

- Cílem je přesvědčit pas, že čtečka může přistupovat k citlivým datům (DG3,DG4)
- Terminál předkládá certifikační řetěz až k cert. CV (ten je uložen v pase)
 - po úspěšném ověření pas získá z certifikátů přístupová práva terminálu (jako AND práv celého cert. řetězce)
 - pas také testuje, zda terminál zná privátní klíč pomocí protokolu typu výzva-odpověď
 - obdoba aktivní autentizace, ale „opačně“
- Použití zjednodušených certifikátů (ne X.509)
- Problém ověření vypršení platnosti certifikátů
 - čip nemá žádné vlastní hodiny
 - nejčerstvější datum vydání korektně ověřeného certifikátu
 - toto datum už určitě nastalo

[Bezpečnost dokumentů I]

- Použití speciálního papíru
 - Bavlna a len (ne celulóza)
 - Žádná bělidla
 - Viditelné pokusy o manipulaci
- S vloženými vlákny



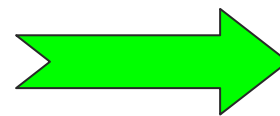
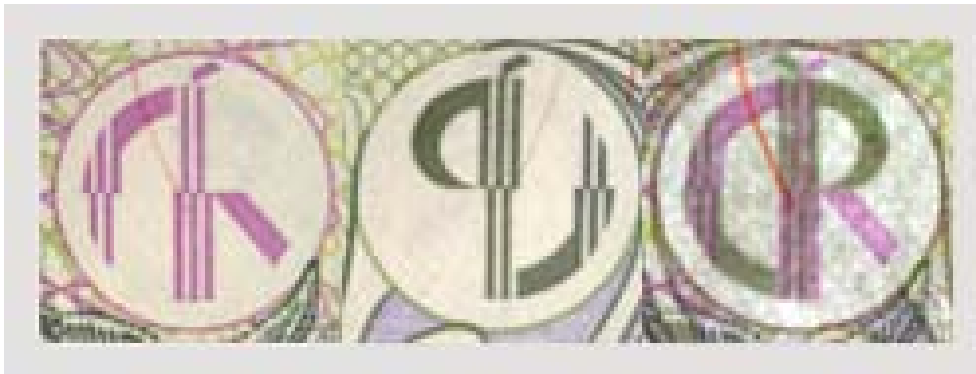
[Bezpečnost dokumentů II]

- Vodoznak
 - Integrovan v papíře
 - Viditelný proti světlu



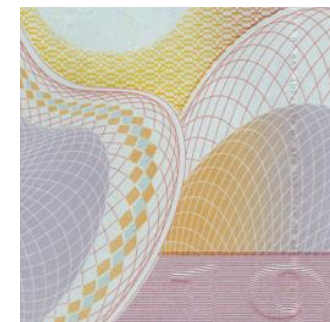
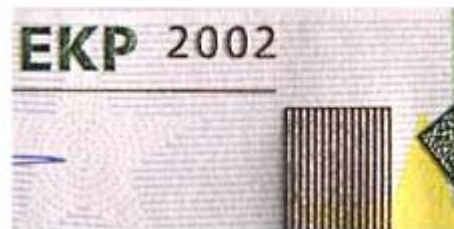
[Bezpečnost dokumentů III]

- Soutisková značka
 - Problém přesného oboustranného tisku



[Bezpečnost dokumentů IV]

- Tiskové techniky
 - hlubotisk
- Mikrotext
- Giloše
- Skryté obrazce



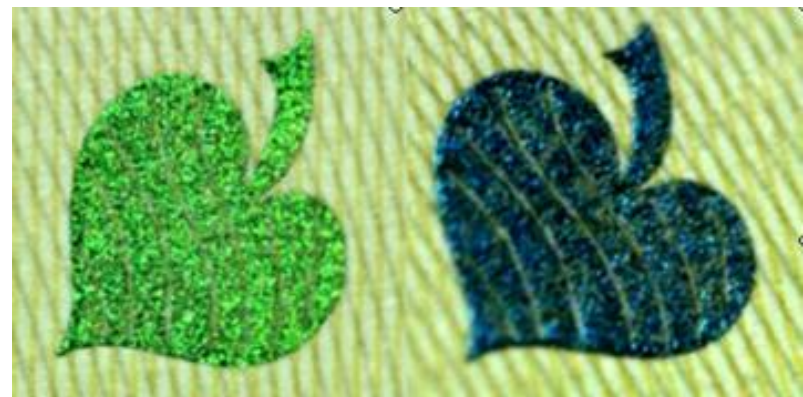
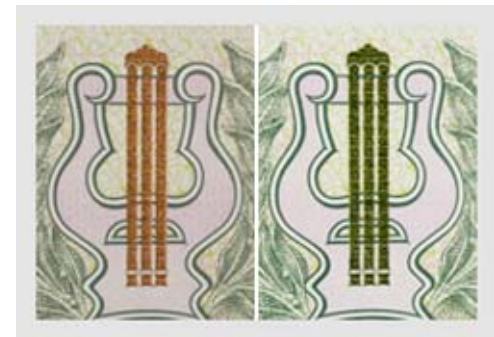
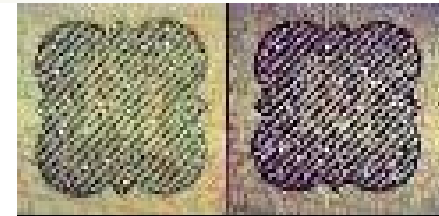
[Bezpečnost dokumentů V]

- Barvy

- Speciální (OVI)

- Mění barvy podle úhlu pohledu

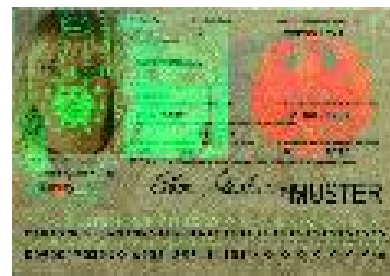
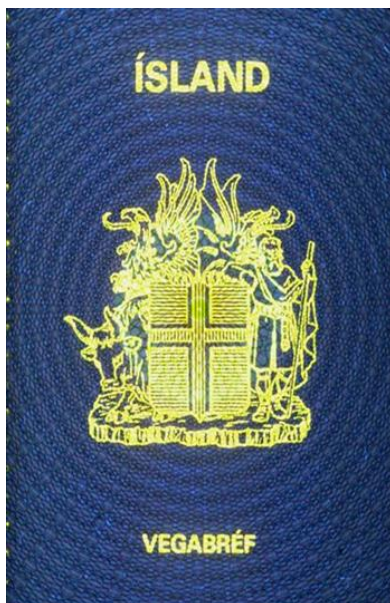
- Duhové



Obrázky pocházejí z PRADO a ČNB

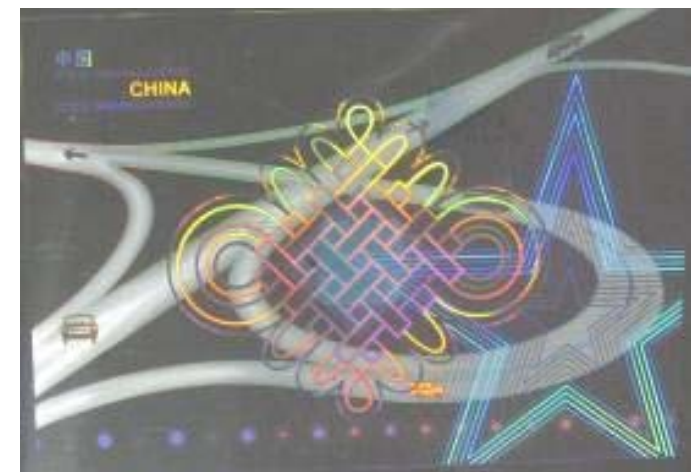
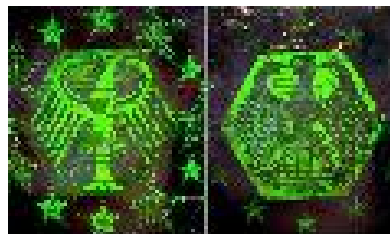
[Bezpečnost dokumentů VI]

- Ultrafialové světlo
 - Papír je tmavý
 - Bělený by zářil
 - Vlákna



[Bezpečnost dokumentů VII]

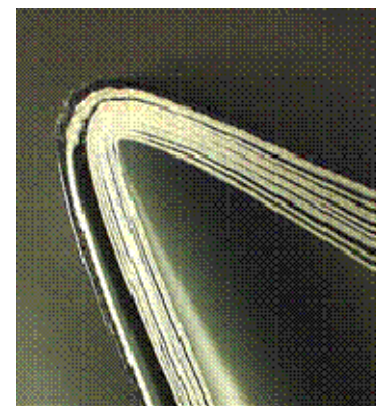
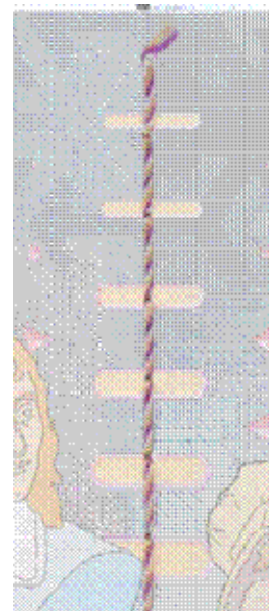
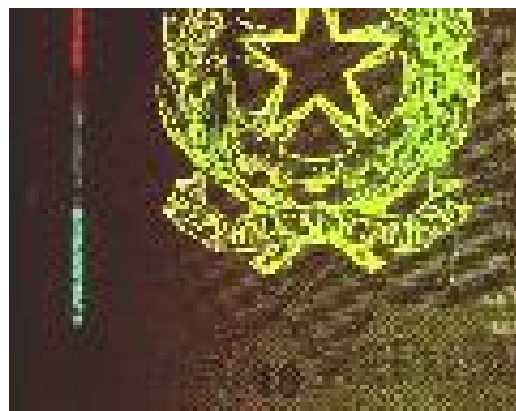
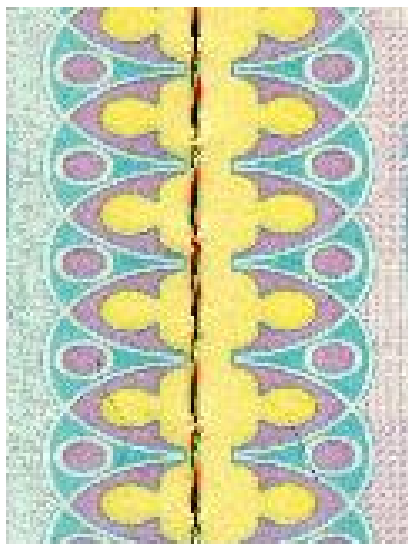
- Hologramy, kinegramy
- OVD (Optically Variable Device)



Obrázky pocházejí z PRADO a VISA

[Bezpečnost dokumentů VIII]

- Vazba dokumentu



[Bezpečnost dokumentů IX]

- Bezpečnostní pásek

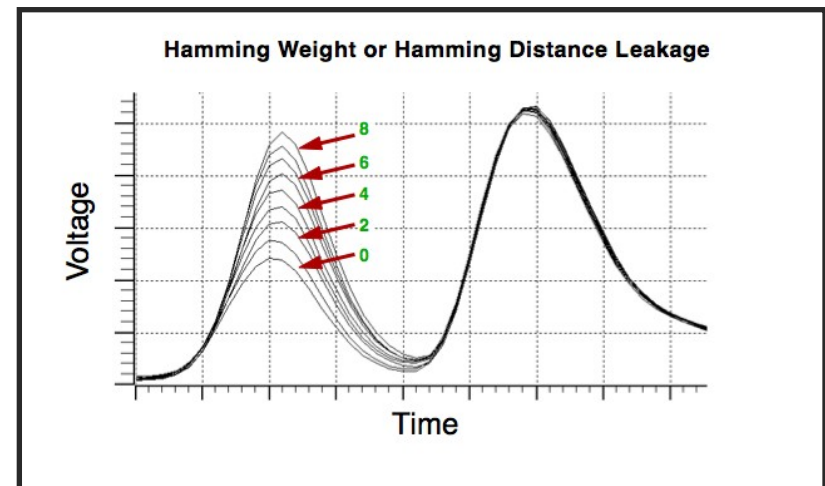
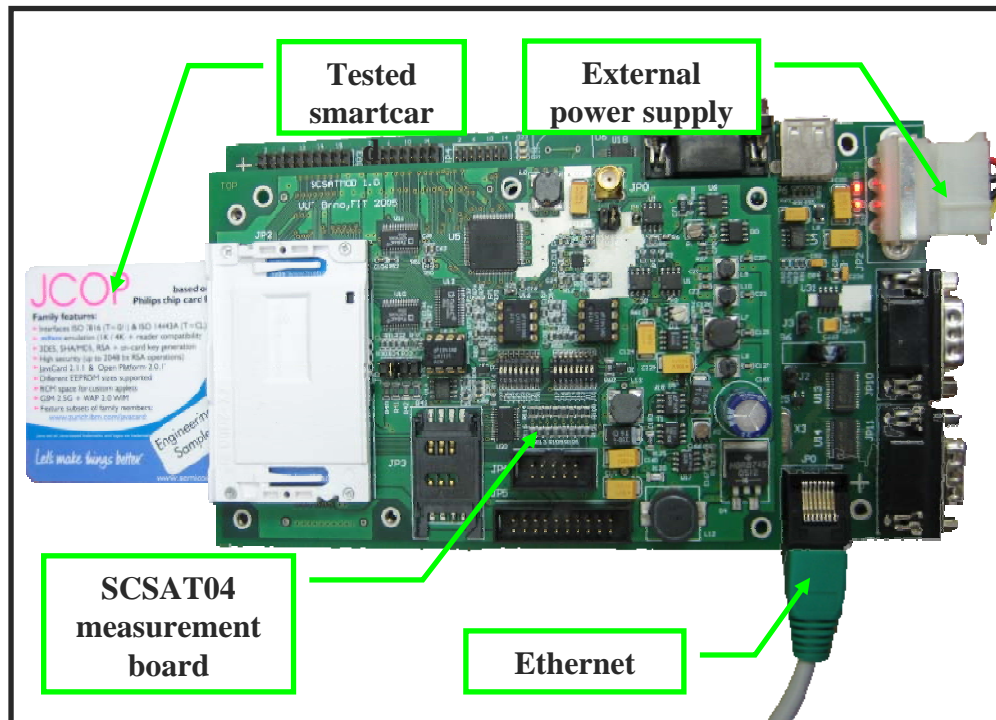


[Labak]

- Laboratoř bezpečnosti a aplikované kryptografie (LaBAK)
- Práce na projektech souvisejících s bezpečností
 - Bezpečnost bezdrátových senzorových sítí (WSN)
 - Bezpečnost čipových karet, mobilů
 - Autentizace (biometriky, tokeny, protokoly)
 - Projekty
 - Grantová agentura a MV ČR
 - Průmysloví partneři – Y Soft, TNS, Cepia Tech., Red Hat, ...

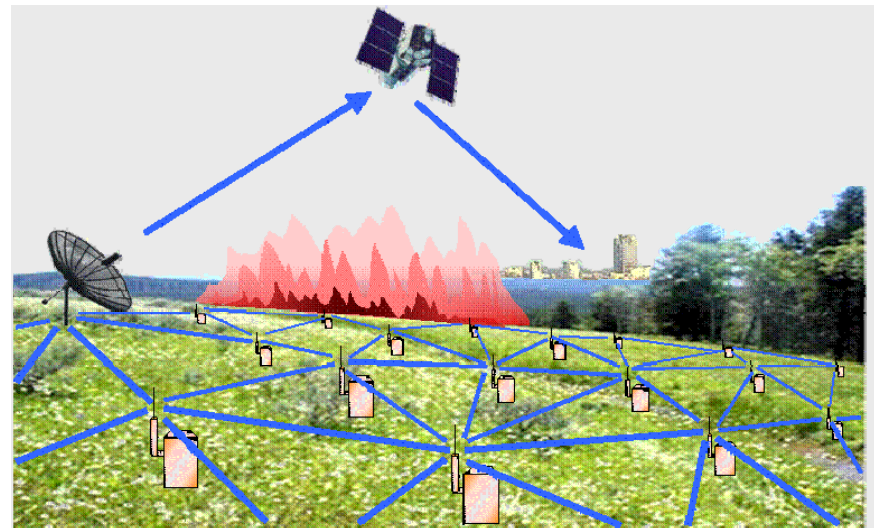
Labak – Oblasti výzkumu I

- Analýza postranních kanálů čipových karet



[Labak – Oblasti výzkumu II]

- Bezdrátové senzorové sítě (WSN)
 - Omezené zdroje
 - Generování bezpečnostních protokolů a strategií útoků
 - IDS systémy
 - Ochrana soukromí



[Labak – závěrečné práce]

<http://www.fi.muni.cz/research/laboratories/labak/topics.xhtml>



Otázky???

Poslední přednáška 15. 5.,
přejeme úspěšné nastudování
a složení zkoušky! 😊